

# Beamforming for Secure Communication via Untrusted Relay Nodes Using Artificial Noise

Siddhartha Sarma

## Abstract

A two-phase beamforming solution for secure communication using untrusted relay nodes is presented. To thwart eavesdropping attempts of relay nodes, we deliberately introduce artificial noise in the source message. After pointing out the incongruity in evaluating secrecy rate in our model for certain scenarios, we provide an SNR based frame work for secure communication. We intend to bring down the SNR at each of the untrusted relay nodes below a certain predefined threshold, whereas, using beamforming we want to boost the SNR at the destination. With this motive optimal scaling vector is evaluated for beamforming phase which not only nullifies the artificial noise transmitted initially, but also maximizes the SNR at the destination. We discuss both the total and individual power constraint scenarios and provide analytical solution for both of them.

## I. INTRODUCTION

Recently omnipresence of wireless devices prompted the researchers and engineers to delve into the security issues of wireless communication. As compared to wired medium, ensuring security for wireless medium is more challenging mainly due to the broadcast nature of the transmission. But the ongoing research on *physical layer security* promises robust and reliable security schemes for wireless communication. Contrary to conventional cryptographic schemes physical layer security techniques are impregnable as the security is ensured by inherent randomness present in the wireless medium.

Physical layer security came to existence through the seminal work of Wyner [1], where he explored the possibility of secure communication without relying on private keys. Later Leung

and Hellman [2] extended this idea to Gaussian channels. Following their works, in last decade several researchers have devised techniques for secure communication in single-hop single and multi-antenna systems. Recently a considerable amount of research is ongoing to extend those schemes to multi-hop network scenarios. In fact, several works have demonstrated that *cooperative relaying* [3, 4] can significantly improve the performance of secure communication. One such cooperative scheme is beamforming, where multiple transmitters adjust their gain and phase to improve the signal strength at the destination. Though beamforming was initially developed for multi-antenna systems, but due to energy and hardware constraints distributed beamforming solution using multiple single antenna node is proposed [3, 4]. In those papers authors have assumed that relay nodes are trustworthy and they beamform towards the destination to defeat (an) external eavesdropper(s). But due to the unprotected nature of public ad hoc network (*e.g.* sensor network), an adversary can wiretap those relay nodes to obtain the information transmitted by source. This prompted us to look for a solution of one of the worst adversarial scenarios of secure communication, where one have to maintain the secrecy of data from the participating relay nodes. Secure transmission using untrusted relay nodes has appeared before in [5–8], where secure communication is obtained by simultaneously transmitting two or more signals. But multiple simultaneous transmission in the above mentioned papers were possible due to multiple sources and/or multiple jammers. In absence of mutiple sources or jammers source has to rely on artificial noise [9]. Authors in [10] considered artificial noise based beamforming solution for AF relay network, but unlike them we have untrusted relay nodes and artificial noise is introduced by the source itself.

In our work we have considered multiple amplify-and-forward (AF) untrusted relay nodes, who help the source to deliver the message at destination, but at the same time can eavesdrop the ongoing transmission. To prevent eavesdropping the source adds artificial noise in the message and broadcast it in first phase. In second phase source and relay nodes beamform to deliver the signal at the destination. Though *secrecy rate* is the conventional metric to evaluate the performance of such system, but for our model in certain scenarios maximizing secrecy rate results in removal of artificial noise. Therefore, we consider a pragmatic approach based on SNR criteria, where we intend keep the SNR at the untrusted relay nodes below certain predefined threshold. Assuming perfect channel state information (CSI), we evaluate the optimal scaling factor for all the transmitting nodes which not only nullifies the artificial noise but also maximizes

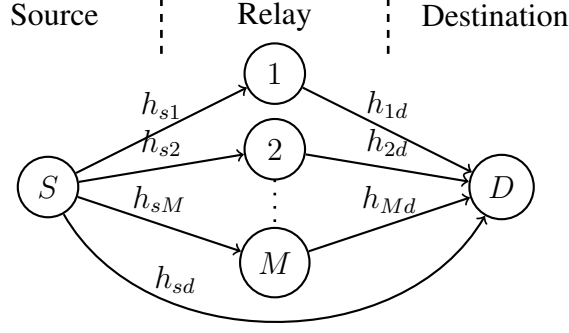


Fig. 1. Simple two hop network with multiple relays

the SNR at the destination. We consider both the total and individual power constraints scenario for all transmitting nodes and provide analytical approach for optimal solutions.

## II. SYSTEM MODEL & PROBLEM FORMULATION

We consider a two-hop network shown in Figure 1 containing multiple relay nodes ( $\mathcal{M} = \{1, 2, \dots, M\}$ ) aiding the transmission from source node  $S$  to destination  $D$ . Adversary is using the relay nodes to passively eavesdrop the on going transmission. To prevent such eavesdropping source transmits artificial noise along with the actual signal to confuse the adversary. In next phase source along with the relay nodes performs beamforming to deliver the message to the destination. We are interested in maximizing the information rate which can be transmitted from the source to the destination securely.

In first phase source transmits a linear combination of two messages  $\sqrt{\alpha P_1}x + \sqrt{(1-\alpha)P_1}u$  using power  $P_1$ , where  $\alpha \in [0, 1]$ ,  $x$  is the Gaussian distributed message with zero mean and unit variance and  $u$  is statistically independent Gaussian distributed artificial noise with identical distribution as  $x$ . The message received at relay and the destination can be written as:

$$y_i = h_{si}(\sqrt{\alpha P_1}x + \sqrt{(1-\alpha)P_1}u) + z_i, i \in \mathcal{M} \cup \{D\}$$

where  $z_i$  are complex Gaussian noise distributed according to  $\mathcal{CN}(0, \sigma^2)$ . In second phase relay nodes along with the source performs beamforming at destination to nullify the artificial noise. In amplify-and-forward (AF) relaying scheme nodes transmit the received noisy message after scaling it by appropriate factor,  $w_i \in \mathbb{C}$ . Source simultaneously transmits  $\sqrt{\alpha P_1}w_0x -$

$\sqrt{(1-\alpha)P_1} \sum_{i=1}^M \frac{w_i h_{si} h_{id}}{h_{sd}} u$ . Therefore, the received message at destination can be written as:

$$y_d = \sqrt{\alpha P_1} (w_0 h_{sd} + \sum_{i=1}^M w_i h_{si} h_{id}) x + \sum_{i=1}^M h_{id} w_i z_i + z_d$$

Assuming Maximum Ratio Combining (MRC) [3], capacity of the source to destination channel can be written as:

$$C_d = \frac{1}{2} \log \left( 1 + \frac{|h_{sd}|^2 \alpha P_1}{\sigma^2 + |h_{sd}|^2 (1-\alpha) P_1} + \frac{|\mathbf{h}^\dagger \mathbf{w}|^2 \alpha P_1}{\sigma^2 (1 + \mathbf{w}^\dagger \mathbf{D}_h \mathbf{w})} \right)$$

where  $\mathbf{w} = [w_0, w_1, \dots, w_M]^\dagger$ ,  $\mathbf{h} = [h_{sd}, h_{s1} h_{1d}, \dots, h_{sM} h_{Md}]^\dagger$ , and  $\mathbf{D}_h$  is  $(M+1) \times (M+1)$  matrix with diagonal elements  $[0, |h_{1d}|^2, |h_{2d}|^2, \dots, |h_{Md}|^2]$ .

As the relays can receive only during the first phase, so the capacity of the source to relay channel is:

$$C_i = \frac{1}{2} \log \left( 1 + \frac{|h_{si}|^2 \alpha P_1}{\sigma^2 + |h_{si}|^2 (1-\alpha) P_1} \right)$$

The total power consumed during the second phase can be calculated in following manner:

$$\alpha P_1 |w_0|^2 + (1-\alpha) P_1 \left| \sum_{i=1}^M \frac{h_{si} h_{id}}{h_{sd}} w_i \right|^2 + \sum_{i=1}^M (|h_{s,i}|^2 P_1 + \sigma^2) |w_i|^2 = \mathbf{w}^\dagger \mathbf{D} \mathbf{w}$$

where  $\mathbf{D} = \begin{bmatrix} \alpha P_1 & \mathbf{0}^t \\ \mathbf{0} & (1-\alpha) P_1 \mathbf{g} \mathbf{g}^\dagger + \mathbf{T} \end{bmatrix}$ ,  $\mathbf{g}$  is  $M$  length vector with  $i^{th}$  element  $g_i = \frac{h_{si} h_{id}}{h_{sd}}$  and  $\mathbf{T}$  is a diagonal matrix with diagonal elements  $[|h_{s,1}|^2 P_1 + \sigma^2, \dots, |h_{s,M}|^2 P_1 + \sigma^2]$ . Therefore, the total power constraint can be expressed as

$$\mathbf{w}^\dagger \mathbf{D} \mathbf{w} \leq P_{tot} \quad (1)$$

For several scenarios individual constraint is more relevant than total constraint. Those constraints can be written as:

$$\mathbf{w}^\dagger \mathbf{D}_s \mathbf{w} \leq P_s \quad (2a)$$

$$|w_i|^2 \leq \frac{P_i}{|h_{si}|^2 P_1 + \sigma^2}, \forall i \in \{1, 2, \dots, M\} \quad (2b)$$

where  $\mathbf{D}_s = \begin{bmatrix} \alpha P_1 & \mathbf{0}^t \\ \mathbf{0} & (1 - \alpha)P_1 \mathbf{g} \mathbf{g}^\dagger \end{bmatrix}$ . Now for a given total or individual power budget maximum achievable secrecy rate can be formulated as following optimization problem:

$$\max \min_i R_{si}(\alpha, \mathbf{w}) = C_d - C_i \quad (3a)$$

Subject to: (1) or (2)

$$\alpha \in [0, 1] \quad (3b)$$

We denote the SNR at  $i^{th}$  relay node as  $\Gamma_i = \frac{|h_{si}|^2 \alpha P_1}{\sigma^2 + |h_{si}|^2 (1 - \alpha) P_1}$ . One can easily see that  $\Gamma_i$  is an increasing function in  $|h_{si}|^2, \forall \alpha \in [0, 1]$ . Therefore, if we order the source to relay channel gains according to their absolute values, then the one with the highest value will have maximum SNR. Formally,

$$\Gamma_e \geq \Gamma_i, \text{ where } e = \arg \max_i [|h_{s1}|^2, \dots, |h_{sM}|^2]$$

Therefore, the objective of the problem (3) can be rephrased as maximize  $C_d - C_e$  for the same constraint set. We rewrite  $C_d - C_e$  in following manner:

$$C_d - C_e = \frac{1}{2} \left[ \log \left( \frac{\rho_d}{\rho_d - \alpha} + f(\mathbf{w}) \alpha \right) - \log \left( \frac{\rho_e}{\rho_e - \alpha} \right) \right]$$

where  $\rho_j = \left( \frac{\sigma^2}{|h_{sj}|^2 P_1} + 1 \right), j \in \{d, e\}$ ,  $f(\mathbf{w}) = \frac{|\mathbf{h}^\dagger \mathbf{w}|^2 P_1}{\sigma^2 (1 + \mathbf{w}^\dagger \mathbf{D}_h \mathbf{w})}$

By differentiating the objective function with respect to  $\alpha$ , we have the following observation.

**Observation.**  $C_d - C_e$  is an increasing function of  $\alpha$  in  $[0, 1]$  if

$$f(\mathbf{w}) \geq \frac{(\rho_d - \rho_e) \rho_d}{(\rho_d - 1)^2 (\rho_e - 2)}$$

assuming  $\rho_e \neq 2$ .

But if we use  $\alpha = 1$ , then in absence of artificial noise, relay nodes can properly decode the message. So, we consider an SNR based approach, where an SNR upto  $\gamma$  results in significant amount of BER in eavesdropping relay nodes and therefore, for all practical purposes we can assume that the message is undecodable at relay nodes. The Optimization problem (3) can be rewritten as:

$$\max C_d \quad (4a)$$

$$\text{subject to: } \Gamma_e \leq \gamma \quad (4b)$$

$$(1) \text{ or } (2), (3b)$$

### III. ANALYSIS & SOLUTION

From the optimization problem (4) one can easily see that to maximize  $C_d$ ,  $\Gamma_e$  should be equal to  $\gamma$ . Therefore, we can calculate the corresponding  $\alpha$  and also using the constraint (3b) we can bound the  $\gamma$  value.

$$\alpha(\gamma) = \frac{1 + \frac{\sigma^2}{|h_{se}|^2 P_1}}{(1 + \frac{1}{\gamma})}, \text{ where } \gamma \leq \frac{|h_{se}|^2 P_1}{\sigma^2}$$

*Total Power Constraint:* Once  $\alpha$  is fixed the first term in the destination SNR is constant, therefore, optimization problem (4) can be reduced to:

$$\max \frac{|\mathbf{h}^\dagger \mathbf{w}|^2}{(1 + \mathbf{w}^\dagger \mathbf{D}_h \mathbf{w})} \quad (5a)$$

$$\text{subject to: } \mathbf{w}^\dagger \mathbf{D} \mathbf{w} \leq P_{tot} \quad (5b)$$

One can check that the constraint will be satisfied with equality at optima and the objective function can be written as:  $\frac{\mathbf{w}^\dagger (\mathbf{h} \mathbf{h}^\dagger) \mathbf{w}}{\mathbf{w}^\dagger \tilde{\mathbf{D}} \mathbf{w}}$ , where  $\tilde{\mathbf{D}} = \frac{1}{P_{tot}} \mathbf{D} + \mathbf{D}_h$ . This is indeed the well known generalized *Rayleigh Quotient problem* [11, p. 176] for which the maximum value of the objective function corresponds to the maximum eigenvalue of matrix  $\tilde{\mathbf{D}}^{-1} \mathbf{h} \mathbf{h}^\dagger$ . The solution can be expressed as  $\mathbf{w}^* = \mu \mathbf{v}$  where  $\mathbf{v} = \tilde{\mathbf{D}}^{-1} \mathbf{h}$  and  $\mu = \sqrt{\frac{P_{tot}}{\mathbf{v}^\dagger \tilde{\mathbf{D}} \mathbf{v}}}$ .

*Individual Power Constraints:* : The individual power constraint problem for AF relaying can be written as:

$$\max \frac{|\mathbf{h}^\dagger \mathbf{w}|^2}{(1 + \mathbf{w}^\dagger \mathbf{D}_h \mathbf{w})} \quad (6a)$$

$$\text{subject to: (2)}$$

It can be seen that the angles of the scaling factors should be chosen in following manner to obtain the optimal value.

$$\arg(w_0) = -\arg(h_{sd}), \arg(w_i) = -(\arg(h_{si}) + \arg(h_{id})), \forall i$$

Therefore, if we denote  $\mathbf{c} = [|h_{sd}|, |h_{s1}|, \dots, |h_{sM}|]^\mathbf{t}$  and  $\mathbf{u} = [|w_0|, |w_1 h_{1d}|, \dots, |w_M h_{Md}|]^\mathbf{t}$ , then the optimization problem (6) can be essentially written as:

$$\max \frac{(\mathbf{c}^\mathbf{t} \mathbf{u})^2}{(1 + \mathbf{u}^\mathbf{t} \mathbf{I}_0 \mathbf{u})} \quad (7a)$$

$$\text{subject to: } \mathbf{u}^\mathbf{t} \hat{\mathbf{D}}_s \mathbf{u} \leq P_s \quad (7b)$$

$$0 \leq u_i \leq u_{max,i}, \forall i \in \mathcal{M} \quad (7c)$$

where  $\mathbf{I}_0 = \begin{bmatrix} 0 & \mathbf{0}^t \\ \mathbf{0} & \mathbf{I} \end{bmatrix}$ ,  $\widehat{\mathbf{D}}_s = \begin{bmatrix} \alpha P_1 & \mathbf{0}^t \\ \mathbf{0} & \frac{(1-\alpha)P_1}{|h_{sd}|^2} \mathbf{h}_s \mathbf{h}_s^t \end{bmatrix}$ ,  $u_{max,i} = \sqrt{\frac{P_i}{|h_{si}|^2 P_1 + \sigma^2}}$ ,  $\mathbf{I}$  is a  $M \times M$  identity matrix, and  $\mathbf{h}_s = [|h_{s1}|, |h_{s2}|, \dots, |h_{sM}|]^t$ .

**Proposition 1.** *The optimal solution for problem (7) with only source constraint i.e. (7b) is given by:  $u_1^* = \sqrt{\eta_1 - \eta_2 \|\mathbf{c}_{(2)}\|^2 r^{*2}}$ ,  $\mathbf{u}_{(2)}^* = \frac{\mathbf{c}_{(2)}}{\|\mathbf{c}_{(2)}\|} r^*$  where  $r^* = \sqrt{\frac{\|\mathbf{c}_{(2)}\|^2 \eta_1}{\|\mathbf{c}_{(2)}\|^4 \eta_2 + (\eta_1 + \|\mathbf{c}_{(2)}\|^2 \eta_2)^2 c_1^2}}$*

*Proof:* We denote the vector  $[u_2, u_3, \dots, u_{M+1}]$  as  $\mathbf{u}_{(2)}$ , then the objective function can be rewritten as:

$$\frac{(c_1 u_1 + \mathbf{c}_{(2)}^t \mathbf{u}_{(2)})^2}{1 + \|\mathbf{u}_{(2)}\|^2}$$

Now it is easy to see that, if  $\|\mathbf{u}_{(2)}\| = r$ , then maximum value of  $\mathbf{c}_{(2)}^t \mathbf{u}_{(2)} = \frac{\mathbf{c}_{(2)}}{\|\mathbf{c}_{(2)}\|} r$ . As the objective function is an increasing function of  $u_1$ , so in absence of individual constraints i.e. (7c), the source constraint (7b) will be satisfied with equality. From that we can calculate the value of  $u_1$  in terms of  $r$ .

$$u_1 = \sqrt{\eta_1 - \eta_2 \|\mathbf{c}_{(2)}\|^2 r^2}, \text{ where } \eta_1 = \frac{P_s}{\alpha P_1}, \eta_2 = \frac{(1-\alpha)}{\alpha |c_1|^2}$$

We can write the objective function (7a) in terms of  $r$  in following manner:  $\frac{(c_1 \sqrt{\eta_1 - \eta_2 r^2} + \|\mathbf{c}_{(2)}\| r)^2}{1 + r^2}$

By differentiating with respect to  $r$  and equating it to 0, we get the above result.  $\blacksquare$

If the solution obtained in the above manner satisfy all the individual constraints, then we have indeed solved the problem (7). But, if for any  $u_i$  individual constraint is violated, then we solve the problem using the following iterative approach.

- 1) Initialize parameters  $t_1 = 0$  and  $t_2 = 1$ .
- 2) Sort the relay nodes in descending order based on  $u_i^*/u_{max,i}$ ,  $\forall i \in \{2, \dots, M\}$ . Sort the vector  $\mathbf{c}_{(2)}$  and  $\mathbf{u}_{max}$  accordingly. In sorted list let us denote the first variable as  $u_{(2)}$ . Update the parameter  $t_1 = t_1 + c_{(2)} u_{(2)}$  and  $t_2 = t_2 + u_{(2)}^2$ . Now we have to solve the following optimization problem:

$$\max \frac{(t_1 + c_1 u_1 + \widehat{\mathbf{c}}^t \widehat{\mathbf{u}})^2}{t_2 + \|\widehat{\mathbf{u}}\|^2} \quad (8a)$$

$$\text{s.t. } \alpha P_1 u_1^2 + \frac{(1-\alpha)P_1}{|h_{sd}|^2} (t_1 + \widehat{\mathbf{c}}^t \widehat{\mathbf{u}})^2 = P_s \quad (8b)$$

where  $\widehat{\mathbf{u}}$  and  $\widehat{\mathbf{c}}$  are the vectors obtained after removing  $u_{(2)}$  and  $c_{(2)}$ , respectively.

- 3) If the solution of problem (8) satisfies all the individual constraints, then optimal solution is obtained, otherwise repeat step 2 & 3 until the solution obtained satisfy their individual constraints.

*Remark:* The rationale behind picking the variable  $u_{(2)}$  corresponding to  $\arg \max_i u_i^*/u_{max,i}$  in step 2 is: for increasing  $P_s$ ,  $u_{(2)}$  is the first variable to violate its individual constraint and (7a) increases with  $u_{(2)}$  till it reaches the optimum corresponding to that  $P_s$  value.

**Proposition 2.** *The optimal solution of the problem (8) is given by  $u_1^* = \sqrt{\eta_1 - \eta_2(t_1 + \|\hat{\mathbf{u}}\|r^*)^2}$ ,  $\hat{\mathbf{u}}^* = \frac{\hat{\mathbf{c}}}{\|\hat{\mathbf{c}}\|}r^*$  where  $r^*$  satisfies the following quadratic polynomial:*

$$q_0r^4 + q_1r^3 + q_2r^2 + q_3r + q_4 = 0 \quad (9)$$

where  $q_0 = \eta_2\eta_3t_1^2\tau^2$ ,  $q_1 = -2\eta_2t_1\tau(\eta_1c_1^2 + \eta_3(t_2\tau^2 - t_1^2))$ ,  $q_2 = \eta_3(\eta_1t_1^2 - \eta_2((t_1^2 - t_2\tau^2)^2 - 2t_1^2t_2\tau^2)) - \eta_1c_1^2(\eta_1 - \eta_2t_1^2 + 2\eta_2t_2\tau^2)$ ,  $q_3 = 2t_1t_2\tau\eta_3(\eta_1 - \eta_2t_1^2 + \eta_2t_2\tau^2)$ ,  $q_4 = t_2^2\tau^2(\eta_1 - \eta_2\eta_3t_1^2)$ ,  $\eta_3 = (1 + \eta_2c_1^2)$ ,  $\tau = \|\hat{\mathbf{c}}\|$

*Proof:* Following the argument of Proposition (1) we can write  $\hat{\mathbf{c}}^t\hat{\mathbf{u}} = \|\hat{\mathbf{c}}\|r$ , where  $\|\hat{\mathbf{u}}\| = r$ . Now due to equality constraint (8b), we can express  $u_1$  in terms of  $r$  as:  $u_1 = \sqrt{\eta_1 - \eta_2(t_1 + \|\hat{\mathbf{c}}\|r)^2}$ . Therefore, optimization problem (8) can be rewritten as:

$$\max_r \frac{(t_1 + \|\hat{\mathbf{c}}\|r + c_1\sqrt{\eta_1 - \eta_2(t_1 + \|\hat{\mathbf{c}}\|r)^2})^2}{t_2 + r^2} \quad (10)$$

By differentiating it with respect to  $r$  and equating it to 0, we get the above polynomial equation in terms of  $r$ . ■

**Corollary 1.** *If  $r^*$  is the real positive root of equation (9) which maximizes the objective function of problem (10), then the solution of problem (8) is obtained using that  $r^*$ .*

*Proof:* As  $u_1$  and  $\hat{\mathbf{u}}$  calculated using  $r^*$  satisfy the constraint (8b) and maximizes (10), hence it is indeed the optimal solution of problem (8). ■

#### IV. RESULTS

In Figure 2 we plot the capacity ( $C_d$ ) of source to destination channel with respect to transmit power at first stage ( $P_1$ ) for multiple  $\alpha$  values. Source to relay and relay to destination channel gains were generated from complex Gaussian distribution with mean 0 and variance 1. The



distribution used for source to destination channel is  $\mathcal{CN}(0, 0.25)$ . While plotting the results we averaged  $C_d$  over 100 such network instances. For individual power constraints we considered  $P_s = 5$  and  $P_i = 0.1, \forall i$ , whereas, for total power constraint we used  $P_{tot} = P_s + M * P_i$ . As the SNR value at the destination is an increasing function of  $P_1$  and  $\alpha$ , so the channel capacity increases as we increase both the parameters. In Figure 3 we plot the capacity for both total

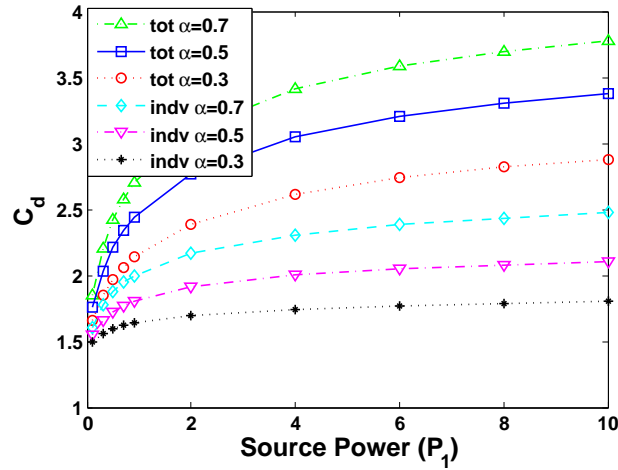


Fig. 2. Plot of  $C_d$  with respect to  $P_1$  for several  $\alpha$  values in case of both total and individual constraints.

and individual constraint scenario with respect to number of the relay nodes. As the number of relay nodes increases the second term in the destination SNR also increases, which results in increase of  $C_d$ .

## V. CONCLUSION

In the current article we have presented a beamforming solution for secure communication using untrusted relay nodes. After justifying SNR based approach, we formulated and solved two optimization problems – one for total power constraint and other for individual power constraints. Our current model assumes a perfect CSI for evaluation of optimal scaling vector which may not be available in several practical scenarios. Therefore, in future we would like to study the performance of our model for delayed CSI.

## REFERENCES

- [1] A. Wyner, “The Wire-tap Channel,” *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan 1975.

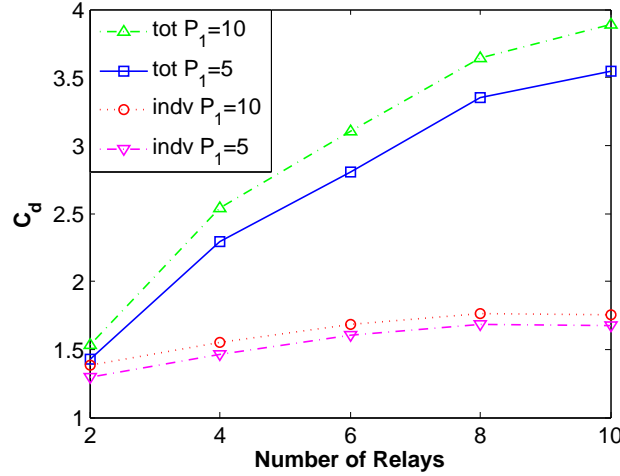


Fig. 3. Plot of  $C_d$  with respect to number of relays for several  $P_1$  values in case of both total and individual constraints.

- [2] S. Leung-Yan-Cheong and M. Hellman, “The Gaussian Wire-tap Channel,” *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul 1978.
- [3] Lun Dong and Zhu Han and Petropulu, A.P. and Poor, H.V., “Amplify-and-forward based cooperation for secure wireless communications,” in *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on*, 2009, pp. 2613–2616.
- [4] J. Zhang and M. C. Gursoy, “Collaborative relay beamforming for secrecy,” in *Communications (ICC), 2010 IEEE International Conference on*. IEEE, 2010, pp. 1–5.
- [5] X. He and A. Yener, “Two-Hop Secure Communication Using an Untrusted Relay: A Case for Cooperative Jamming,” in *IEEE Global Telecommunications Conference (GLOBECOM 08)*, Dec 2008, pp. 1–5.
- [6] R. Zhang, L. Song, Z. Han, B. Jiao, and M. Debbah, “Physical Layer Security for Two Way Relay Communications with Friendly Jammers,” in *IEEE Global Telecommunications Conference (GLOBECOM 2010)*, Dec 2010, pp. 1–6.
- [7] C. Jeong, I.-M. Kim, and D. I. Kim, “Joint secure beamforming design at the source and the relay for an amplify-and-forward mimo untrusted relay system,” *IEEE Transactions on Signal Processing*, vol. 60, no. 1, pp. 310–325, Jan 2012.
- [8] X. He and A. Yener, “Cooperation with an Untrusted Relay: A Secrecy Perspective,” *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3807–3827, 2010.

- [9] R. Negi and S. Goel, “Secret Communication using Artificial Noise,” in *Proceeding IEEE 62nd Vehicular Technology Conference (VTC-2005-Fall)*, vol. 3, Sep 2005, pp. 1906–1910.
- [10] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and M. Lin, “Optimal Joint Cooperative Beamforming and Artificial Noise Design for Secrecy Rate Maximization in AF Relay Networks,” in *IEEE 14th Workshop on Signal Processing Advances in Wireless Communications (SPAWC), 2013*, June 2013, pp. 360–364.
- [11] R. A. Horn and C. R. Johnson, Eds., *Matrix Analysis*. New York, NY, USA: Cambridge University Press, 1986.